



PASS THE WORD Cyber Security Now More Important Than Ever

Everybody knows that passwords are necessary to keep prying eyes away from sensitive online information. And exactly nobody likes keeping track of passwords or, worse, being prompted to change them often. When it comes to personal accounts such as credit cards, email, banking, etc., the amount of risk we feel comfortable taking will dictate how conscientious we are about using complex passwords, using different passwords for different accounts, and changing them frequently.

But in our work life, we don't have that luxury. The stakes are orders of magnitude higher than just being locked out of our Netflix account. The harm that bad actors can inflict on a business is nearly incalculable. Lackadaisical management of passwords can result in a catastrophe that costs a business millions of dollars and untold embarrassment. Hackers, as is their custom, are becoming wilier every day, constantly dreaming up new ways to break through what we wrongly consider the impenetrable firewall that protects our information.

Healthcare in the Crosshairs

The healthcare industry has become an attractive target for cybercriminals. IBM [says](#) that data breach costs in 2021 rose to \$4.24 million. With the burgeoning use of electronic health records (EHRs), the numbers of potential targets is in the many millions. In addition to protected health information (PHI), which must be guarded at all costs, there is critical financial information residing on the computers of even the smallest healthcare facilities. *Healthcare IT News* [reported](#) that as of November 2021, more than 40 million patient records had been compromised by incidents reported to the federal government in 2021.

Chief Information Security Officers in healthcare settings do have some weapons at their disposal to counter unauthorized attempts to gain access. These include complex passwords, Single Sign-On (SSO), and Multifactor Authentication (MFA).

Complex Passwords, SSO, and MFA

The idea of **complex passwords** is simple. The creation of passwords of at least 16 characters that include random uppercase and lowercase letters, numbers, and symbols makes it hard for hackers to penetrate. Unfortunately, it also makes it hard for a facility's employees to keep track of. And when employees are using a variety of devices such as desktop computers, laptops, cellphones, tablets, juggling these passwords for different applications becomes that much more difficult.

Single Sign-On

Is an authentication service that allows an end user to employ one set of login credentials, such as a username and password, for multiple applications. Enterprise Single Sign-On provides software and services to store and transmit encrypted user credentials across local and network boundaries. The benefit to users is that they no longer have to remember or look up different credentials for different applications. The risk is that SSO presents a single point of failure that attackers can exploit. In addition, some applications might require additional levels of security, and users could be locked out of other apps if they are unable to access the primary account or app.

We're all familiar with **Multifactor Authentication** in our personal online lives. Banks, physicians' offices and other institutions with which we do business often ask us to receive a time-limited code via text message or email even after we have properly attempted to log in with our username and password. Once we input the code, we're in. In the healthcare setting, MFA provides an extra layer of protection, especially when used in tandem with SSO.

Shutting Off Access Quickly is Key

But even after instituting these safeguards, health systems still face potential risks. Are employees accessing insurance company websites (aka payor portals) for which they are not authorized? Do former employees still have access to these sites? Will current employees still need to juggle passwords? Questions like these have prompted many facilities to turn to healthcare specialists like ZYNC to protect their critical relationships with payors.

ZYNC's password auto-encryption capability removes all unnecessary payor portal user access, rendering access to ePHI controlled and auditable. And when an employee leaves an organization, access to sensitive portals can be turned off with one click, preventing unauthorized use after termination. In addition, administrators no longer need to worry about locked accounts and forgotten passwords. ZYNC manages the passwords and saves hours of repetitive reset and reinstatement.

The ZYNC dashboard also provides insight into which users have weak passwords and suggests ways to strengthen them. Especially in these times of staff shortages when administrators' time is even more precious, it makes economic sense to hand over this important task to the experts.